

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-341223
 (43)Date of publication of application : 22.12.1998

(51)Int.Cl.

H04L 9/14

(21)Application number : 09-150947

(71)Applicant : HITACHI LTD

(22)Date of filing : 09.06.1997

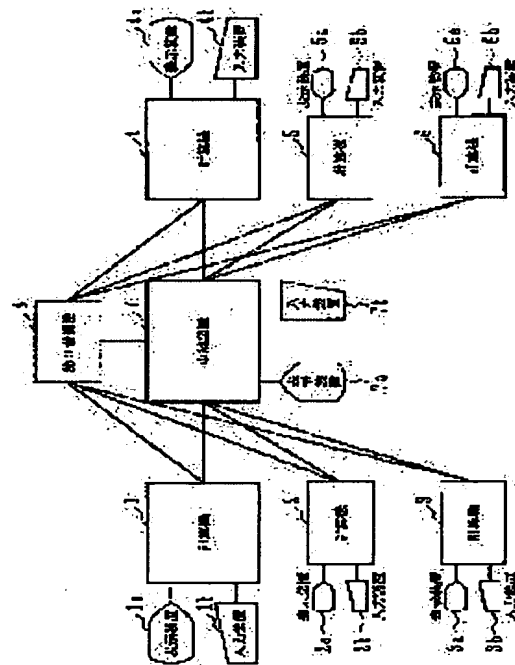
(72)Inventor : SAITO MAKOTO

(54) ENCRYPTION COMMUNICATION SYSTEM AND ENCRYPTION COMMUNICATION REPEATER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the encryption communication system and encryption communication repeater where troublesome processing of keys for a transmitter computer conducting encryption communication is not required, consumption of a memory capacity for storing the keys is avoided, and key management required for encryption communication among lots of computers is conducted efficiently.

SOLUTION: A repeater 7 is introduced between computers 1, 14 that conduct mutual encryption communication, the repeater 7 stores a common key between the transmitter computer 1 and the receiver computer 4, an encrypted message from the transmitter computer 1 is decoded and encrypted with a common key to the receiver computer 4 and the encrypted message is sent to the receiver computer 4. Thus, the transmitter computer 1 manages only the common key to the repeater 7 to make the encryption communication with lots of destination computers 4-7 thereby facilitating the key management.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-341223

(43) 公開日 平成10年(1998)12月22日

(51) Int.Cl.⁶
H 0 4 L 9/14

識別記号

F I
H 0 4 L 9/00

6 4 1

審査請求 未請求 請求項の数12 O L (全 21 頁)

(21) 出願番号 特願平9-150947

(22) 出願日 平成9年(1997)6月9日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 齋藤 誠

神奈川県横浜市都筑区加賀原二丁目2番

株式会社日立製作所ビジネスシステム開発
センタ内

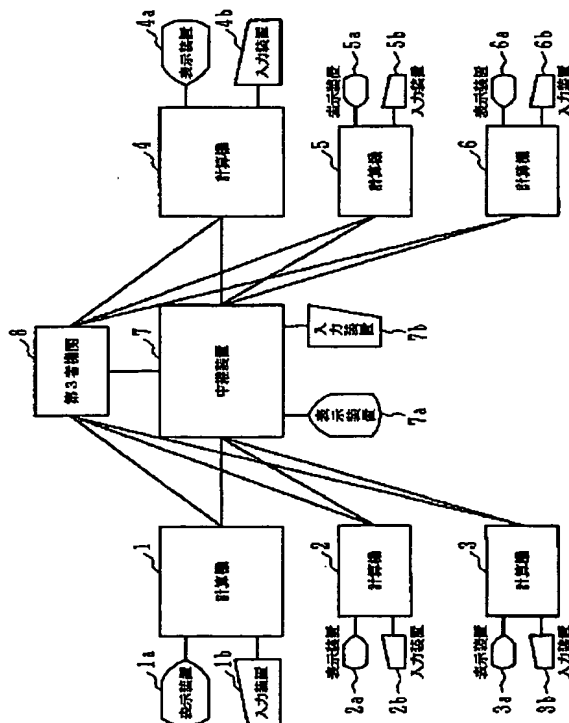
(74) 代理人 弁理士 磯村 雅俊

(54) 【発明の名称】 暗号通信システムおよび暗号通信中継装置

(57) 【要約】

【課題】 多数の相手先計算機との高速な暗号通信をするためには送信側計算機での鍵の取り扱いが煩雑となり、かつ鍵保管にメモリ容量を消費してしまう。

【解決手段】 相互に暗号通信する計算機1、4間に、中継装置7を導入し、この中継装置7で、送信計算機1および受信計算機4との共通鍵を保持し、送信計算機1からの暗号化メッセージを復号化し、受信計算機4との共通鍵で暗号化して受信計算機4に送信することにより、送信側計算機1では、中継装置7との共通鍵のみを管理するだけで、多数の相手先計算機4～6との暗号通信ができ、鍵管理が容易となる。



【特許請求の範囲】

【請求項1】 メッセージを暗号化して計算機間での通信を行う暗号通信システムにおいて、送信側計算機からの暗号メッセージを受信して復号化し、該復号化したメッセージを、受信側計算機に暗号化して送信する中継装置を設けることを特徴とする暗号通信システム。

【請求項2】 請求項1に記載の暗号通信システムにおいて、上記中継装置は、上記送信側計算機および上記受信側計算機との各共通鍵を保持し、上記送信側計算機から受信した上記暗号メッセージを上記送信側計算機との共通鍵で復号化し、該復号化したメッセージを、上記受信側計算機との共通鍵で暗号化して上記受信側計算機に送信することを特徴とする暗号通信システム。

【請求項3】 請求項2に記載の暗号通信システムにおいて、暗号通信をする計算機を追加する毎に、該追加した計算機と上記中継装置で用いる上記共通鍵を、上記追加した計算機と上記中継装置に通知する第3者機関を設けることを特徴とする暗号通信システム。

【請求項4】 請求項2に記載の暗号通信システムにおいて、上記計算機および上記中継装置からの要求に基づき、上記共通鍵を、要求元の上記計算機および上記中継装置に通知する第3者機関を設けることを特徴とする暗号通信システム。

【請求項5】 請求項1に記載の暗号通信システムにおいて、上記中継装置は、1対の公開鍵と秘密鍵、および、上記受信側計算機の公開鍵を保持し、上記送信側計算機から上記1対の公開鍵で暗号化されたメッセージを受信して上記1対の秘密鍵を用いて復号化し、該復号化したメッセージを、上記受信側計算機の公開鍵を用いて暗号化して上記受信側計算機に送信することを特徴とする暗号通信システム。

【請求項6】 請求項5に記載の暗号通信システムにおいて、上記送信側計算機からの要求に基づき、上記1対の公開鍵を上記送信側計算機に通知する第3者機関を設け、上記送信側計算機は、上記第3者機関から通知された上記1対の公開鍵を用いて上記メッセージを暗号化して上記中継装置に送出することを特徴とする暗号通信システム。

【請求項7】 請求項1から請求項6のいずれかに記載の暗号通信システムにおいて、複数の上記中継装置のそれぞれの上記受信側計算機との通信量を平準化するよう、上記複数の中継装置の上記受信側計算機との接続組み合わせを制御する接続管理手段を設けることを特徴とする暗号通信システム。

【請求項8】 請求項1から請求項7のいずれかに記載の暗号通信システムにおいて、複数の上記中継装置の各々の上記受信側計算機との通信量が少ない接続を優先して選択し、該選択した接続先の上記受信側計算機を他の上記中継装置との接続に切替る接続切替手段を設けることを特徴とする暗号通信システム。

【請求項9】 請求項1から請求項8のいずれかに記載の暗号通信システムにおいて、複数の上記中継装置のそれぞれの上記受信側計算機との接続状況に基づき、上記送信側計算機と接続する上記中継装置を決定する接続制御手段を設けることを特徴とする暗号通信システム。

【請求項10】 請求項1から請求項9のいずれかに記載の暗号通信システムにおいて、上記送信側計算機と上記受信側計算機との暗号通信に用いる同じ暗号鍵を、複数の上記中継装置のそれぞれに保持させ、任意の中継装置で、上記送信側計算機と上記受信側計算機との暗号通信の中継を行なうことを特徴とする暗号通信システム。

【請求項11】 請求項1から請求項9のいずれかに記載の暗号通信システムにおいて、複数の上記中継装置が共有するメモリに、上記送信側計算機と上記受信側計算機との暗号通信に用いる全ての暗号鍵を保持し、任意の中継装置で、上記送信側計算機と上記受信側計算機との暗号通信の中継を行なうことを特徴とする暗号通信システム。

【請求項12】 メッセージを暗号化して計算機間での通信の中継を行う暗号通信中継装置であって、送信側計算機からの暗号メッセージを受信して復号化する手段と、該復号化したメッセージを、受信側計算機に暗号化して送信する手段とを具備することを特徴とする暗号通信中継装置。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、共通鍵や公開鍵などの暗号鍵を用いてメッセージを暗号化し、計算機間での通信を行う暗号通信技術に係り、特に、多数の計算機間での暗号通信を効率的に行うのに好適な暗号通信システムおよび暗号通信中継装置に関するものである。

【0002】

【従来の技術】計算機（コンピュータ）間でメッセージを暗号化して通信する場合には、例えば、電子情報通信学会編「電子情報通信ハンドブック」（1988年、オーム社発行）の第1944、1945頁に記載のように、共通鍵や公開鍵などの暗号鍵を用いる。共通鍵を用いる場合は、送受信の両方の計算機で同じ暗号鍵（共通鍵）を保持し、その共通鍵を用いてメッセージの暗号化と復号化を行う。また、公開鍵を用いる場合は、送信側計算機でメッセージを公開鍵で暗号化し、受信側計算機では、受信した暗号化メッセージを、公開鍵と対をなす秘密鍵で復号化する。

【0003】従来の暗号通信技術では、送信側計算機が、受信側計算機との共通鍵、あるいは、受信側計算機の公開鍵を予め取得しておき、これらの共通鍵や公開鍵を用いてデータ（メッセージ）を暗号化し、受信側計算機に送信していた。しかし、この技術では、多数の受信側計算機との共通鍵、あるいは、多数の受信側計算機の公開鍵を保持する必要があるため、鍵の取り扱いが煩雑とな

るとの問題や、鍵保管のためのメモリ容量が多く必要になる等の問題がある。例えば、ＩＣカードを用いたエレクトロニックコマース（電子商取引）を実現する場合、暗号によるコンピュータセキュリティの知識が乏しい一般ユーザが暗号鍵を取扱う必要があるが、従来の暗号通信システムでは、多くの暗号鍵が必要であり、十分安全に管理できない恐れや、暗号鍵格納のためにＩＣカードのメモリを浪費してしまう。

【０００４】このような問題に対処するために、例えば、「Secure Socket Layer」プロトコルのハンドシェイクプロトコル等に従って通信することで共通鍵を共有する技術や、送信側計算機が受信側計算機に公開鍵を要求することで、送信側計算機が公開鍵を得る技術等のように、通信の必要が発生した時に取得する技術が開示されている。しかし、この技術においては、通信の必要発生時に送信側計算機が暗号鍵を得るため、暗号通信完了までに時間がかかるといった問題がある。

【０００５】

【発明が解決しようとする課題】解決しようとする問題点は、従来の技術では、暗号通信をする送信側計算機では、多数の受信側計算機との共通鍵、あるいは、多数の受信側計算機の公開鍵を保持する必要がある点と、暗号通信完了までに時間がかかってしまう点である。本発明の目的は、これら従来技術の課題を解決し、暗号通信をする送信側計算機での煩雑な鍵の取り扱いを不要とし、かつ、鍵保管のためのメモリ容量の消費を回避し、多数の計算機間での暗号通信に必要な鍵管理を効率良く行うことを可能とする暗号通信システムおよび暗号通信中継装置を提供することである。

【０００６】

【課題を解決するための手段】上記目的を達成するため、本発明の暗号通信システムおよび暗号通信中継装置では、計算機間での暗号通信を、中継装置を介して行う。すなわち、中継装置は、通信相手の公開鍵、あるいは、通信相手との共通鍵を予め保持し、送信側計算機からの暗号メッセージを復号化し、復号化したメッセージを受信側計算機の暗号鍵で暗号化して受信側計算機へ送信することにより、送信側計算機は、中継装置との共通鍵、あるいは、中継装置の公開鍵のみを持てば良くなり、予め保持しても、鍵の管理負担が小さくなると共に、通信の必要発生時に暗号鍵を得る技術に比べて、暗号通信完了までの時間が短くなる。

【０００７】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図１は、本発明の暗号通信システムおよび暗号通信中継装置の本発明に係る構成の一実施例を示すブロック図である。本図１において、１～６は相互に暗号通信を行う計算機、７は各計算機１～６間の暗号通信を仲介する暗号通信中継装置としての中継装

置、８は各計算機１～６と中継装置７が暗号通信するための共通鍵を発行する鍵管理センタとしての第３者機関である。各計算機１～６と中継装置７のそれぞれには、ＣＲＴ（Cathode Ray Tube）等からなり画面を表示する表示装置１ａ～７ａと、キーボード等からなりデータを入力する入力装置１ｂ～７ｂが設けられている。

【０００８】以下、このような構成での本発明に係る処理の概略を、計算機１と計算機４との通信を例に説明する。まず、各計算機１、４が中継装置７と暗号通信するためのそれぞれの共通鍵を、第３者機関８から計算機１、４、および、中継装置７に配布する手順を説明する。尚、本手順は、「Kerberos」と呼ばれるものである。また、この鍵の配布の契機としては、暗号通信システムに計算機１、４を接続した時、直ちに行なうことでも、あるいは、取引の必要が生じた時に行なうことでも良い。

【０００９】第３者機関８は、自分（第３者機関８）と中継装置７との共通鍵で暗号化されたチケットと、計算機１と中継装置７との共通鍵とが中に入った証明書を、計算機１と第３者機関８との共通鍵で暗号化し、計算機１に送る。計算機１は、第３者機関８から送られてきた証明書を、第３者機関８との共通鍵で復号化し、チケットと共通鍵を取り出し、チケットを中継装置７に送る。中継装置７は、計算機１から送られてきたチケットを、第３者機関８から送られてきた第３者機関８との共通鍵で復号化し、中から、計算機１のユーザ名、ユーザのログイン名、および、計算機１との共通鍵を取り出す。

【００１０】次に、計算機４と中継装置７がお互いに暗号通信するための共通鍵を得る手順を説明する。第３者機関８は、中に、自分（第３者機関８）と中継装置７との共通鍵で暗号化されたチケットと、計算機４と中継装置７との共通鍵が入った証明書を、計算機４と第３者機関８との暗号鍵で暗号化し、計算機４に送る。計算機４は、第３者機関８から送られてきた証明書を、第３者機関８との共通鍵で復号化し、チケットと共通鍵を取り出し、チケットを中継装置７に送る。中継装置７は、計算機４から送られてきたチケットを、第３者機関８から送られてきた第３者機関８との共通鍵で復号化し、中から、計算機４を使用するマーチャント名、マーチャントのログインＩＤ、および、計算機４との共通鍵を取り出す。以上の手順により、計算機１と中継装置７、および、中継装置７と計算機４は共通鍵を共有する。

【００１１】次に、計算機１と計算機４が、中継装置７を中継して暗号通信する手順を説明する。まず、計算機１は、データを中継装置７との共通鍵で暗号化し、中継装置７に送る。中継装置７は、受信したデータを計算機１との共通鍵を用いて復号化し、計算機４との共通鍵で暗号化して計算機４に送る。計算機４は、受信したデータを中継装置７との共通鍵で復号化し、データを処理する。このようにして、中継装置７を中継しての暗号通信

が行われる。尚、逆向きの通信も同様にして可能である。また、ここでは、データを暗号化する暗号鍵として、共通鍵を例にして説明しているが、共通鍵でなく公開鍵でも良い。この場合、復号には秘密鍵を用いる。そして、このように暗号鍵として公開鍵を使用する場合、中継装置7の公開鍵を、計算機1あるいは計算機4に予め通知しておく。

【0012】次に、図2を用いて、図1における暗号通信システムおよび暗号通信中継装置の本発明に係る構成およびその処理動作を詳しく説明する。図2は、図1における計算機と中継装置および第3者機関のそれぞれの内部構成例を示すブロック図である。まず、計算機1と中継装置7、および、中継装置7と計算機4が、共通鍵を共有する手順を説明する。

【0013】第3者機関8内の証明書作成部8bは、鍵管理テーブル8aから、第3者機関8と計算機1の或るユーザの共通鍵と、計算機1の或るユーザと中継装置7との共通鍵、第3者機関8と中継装置7との共通鍵、ユーザ名、ユーザのログイン名、および、ユーザのメールアドレスを読み出し、これらのユーザ名、ユーザのログイン名、計算機1の或るユーザと中継装置7との共通鍵から、チケットを作成し、このチケットを第3者機関8と中継装置7の共通鍵で暗号化する。次に、証明書作成部8bは、暗号化したチケットと、計算機1の或るユーザと中継装置7の共通鍵とから、証明書を作り、この証明書を、第3者機関8と計算機1の或るユーザとの共通鍵で暗号化する。そして、オペレータの操作に基づき、第3者機関8は、メール処理部8cにより、暗号化した証明書を、計算機1のメール処理部1cに送る。

【0014】計算機1では、ユーザによるOS（オペレーションシステム）1jのエディタ等を使つての操作に基づき、鍵管理テーブル1h中の自分（或るユーザ）と第3者機関8との共通鍵を、自分のログインIDをキーに読み出し、復号化部1gに入力する。復号化部1gは、入力された共通鍵を用いて、メール処理部1cで受け取った第3者機関8からの証明書を復号化する。そして、計算機1は、復号化した証明書から、チケットと、中継装置7と自分の共通鍵とを取り出し、取り出した共通鍵と自分のログインIDを鍵管理テーブル1hに登録し、チケットを、ユーザからの操作に基づき、メール処理部1cにより、中継装置7のメール処理部7cに送る。

【0015】中継装置7では、オペレータによるOS7jのエディタ等を使つての操作に基づき、鍵管理テーブル7h中の自分と第3者機関8との共通鍵を、オペレータのログインIDをキーに読み出し、復号化部7gに入力する。復号化部7gは、入力された共通鍵を用いて、メール処理部7cで第3者機関8から受け取ったチケットを復号化する。そして、中継装置7は、復号化したチケットから、ユーザ名、ユーザのログインID、計算機

1の或るユーザと中継装置7との共通鍵を取り出し、取り出した共通鍵と中継装置7のオペレータのログインIDとを鍵管理テーブル7hに登録する。また、ユーザ名とユーザのログインIDの組みを、ユーザ名／マーチャント名変換テーブル7kに登録する。

【0016】同様にして、中継装置7は、計算機4を使用するマーチャントとの共通鍵と、そのマーチャント名、および、ログインIDを得、また、計算機4を使用するマーチャントは、中継装置7との共通鍵を得る。そして、計算機4のマーチャントは、自分のログインIDと、中継装置7との共通鍵を鍵管理テーブル4hに登録する。また、中継装置7では、オペレータの操作に基づき、マーチャント名とマーチャントのログインIDの組みを、ユーザ名／マーチャント名変換テーブル7kに登録し、マーチャントの部分を、送られてきた鍵で暗号化し、計算機4に送る。計算機4では、送られてきたマーチャントの部分を復号化し、マーチャント名テーブル4kに登録し、そして、マーチャントのログインIDと、マーチャントとの共通鍵を鍵管理テーブル7hに登録する。

【0017】このような状態において、計算機1が中継装置7を介して計算機4と暗号通信を行う手順を、次に説明する。計算機1のユーザは、計算機1にログインIDを入力し、ログインする。次に、業務処理部1dを起動し、ユーザ名と、取引したいマーチャント名を入力する。これに基づき、業務処理部1dは、暗号通信処理部1eに、中継装置7とのコネクション確立要求を発行する。暗号通信処理部1eは、このコネクション確立要求を受けると、ユーザのログインIDをシステムファイルから読み出し、コネクションIDを生成し、読み出したユーザのログインIDをキーに鍵管理テーブル1hから中継装置7との共通鍵を読み出し、コネクション管理テーブル1iを作成する。さらに、計算機1は、コネクション確立要求にパラメータをセットし、暗号化部1fで暗号化した後、暗号通信処理部1eを介して、中継装置7に送信する。このコネクション要求には、ユーザ名、ユーザのログインID、コネクションID、マーチャント名が含まれる。

【0018】中継装置7は、暗号通信処理部7eで、計算機1からのコネクション確立要求を受信すると、ユーザ名／マーチャント名変換テーブル7kから、ユーザ名をキーにログインIDを検索し、さらに、これから共通鍵を求めて、復号化部7gで、コネクション確立要求メッセージを復号化する。また、ユーザ名／マーチャント名変換テーブル7kでマーチャントのログインIDを検索した後、マーチャント側コネクションIDを生成し、コネクション管理テーブル7iを作成する。そして、コネクション確立要求にパラメータをセットし、暗号化部7fで暗号化した後、計算機4のマーチャントに送る。また、同様に暗号化したコネクション確立応答を計算機

1に送る。計算機4に送るコネクション確立要求には、マーチャント側コネクションID、マーチャント名、ログインIDが含まれ、また、計算機1に送るコネクション確立応答には、ユーザ側コネクションIDが含まれる。

【0019】このようにして中継装置7から送られてきたコネクション確立要求を、暗号通信処理部4eで受信すると、計算機4は、マーチャント名変換テーブル4kからログインIDを探し、このログインIDから、共通鍵を検索して、この共通鍵を復号化部4fで復号化する。そして、コネクション管理テーブル4iを作成し、コネクション確立応答を、暗号化部4fで暗号化し、中継装置7に返す。尚、このコネクション確立応答には、マーチャント側コネクションIDが含まれる。このようにして、中継装置7を介しての計算機1、4間のコネクションが確立される。

【0020】以下、このようにしてコネクションが確立された計算機1、4間での通常のデータ通信に関して説明する。計算機1のユーザが入力したメッセージには、コネクションIDが付加され、暗号化部7fで暗号化され、中継装置7の暗号通信処理部7eに送られる。中継装置7においては、受信したメッセージは、コネクション管理テーブル7iを基に復号化部7gで復号化された後、マーチャント側コネクションIDが付加され、さらに、暗号化部7fで暗号化した後、計算機4の暗号通信処理部4eに送られる。

【0021】計算機4では、中継装置7から送られてきたメッセージは、コネクション管理テーブル4iに基づいて復号化部4fで復号化された後、業務処理部4dに渡される。返り電文も同様である。すなわち、計算機1と中継装置7間のメッセージには、ユーザ側コネクションIDが付加され、計算機4と中継装置7間のメッセージには、マーチャント側コネクションIDが付加され、これらのIDとコネクション管理テーブル1i、4i、7iを照合することで電文を制御する。

【0022】次に、図3～図17を用いて、コネクション管理テーブル1i、4i、7iと鍵管理テーブル1h、4h、7h、および、マーチャント名変換テーブル4k、ユーザ名／マーチャント名変換テーブル7の各テーブルの構造を説明し、その後で、図18～図20の各フローチャートにより、中継装置7を用いた暗号通信の詳細な動作を説明する。

【0023】図3は、図2における発信側計算機の鍵管理テーブルの詳細な構成例を示す説明図である。図2における計算機1の鍵管理テーブル1hには、ユーザ(1)鍵情報、ユーザ(2)鍵情報、ユーザ(3)鍵情報、・・・、ユーザ(n)鍵情報等の、計算機1の各ユーザ毎のログインIDと共通鍵が登録される鍵情報エリア(領域)1h1～1hnが設けられている。

【0024】図4は、図3の鍵管理テーブルにおける任

意のユーザの鍵情報エリアの詳細な構成例を示す説明図である。一つの鍵情報エリア1hxは、それぞれ、ユーザ(x)のログインID、ユーザ(x)と第3者機関の共通鍵、ユーザ(x)と中継装置の共通鍵が登録される項目欄1hx1～1hx3から構成されている。

【0025】図5は、図2における中継装置の鍵管理テーブルの詳細な構成例を示す説明図である。図2における中継装置7の鍵管理テーブル8aには、中継装置の鍵情報が登録される鍵情報エリア8a1と、ユーザ(1)～(n)のそれぞれの鍵情報が登録される鍵情報エリア8a2a～8a2n、および、マーチャント(1)～(m)のそれぞれの鍵情報が登録される鍵情報エリア8a3a～8a3mが設けられている。

【0026】図6は、図5の鍵管理テーブルにおける中継装置の鍵情報エリアの詳細な構成例を示す説明図である。中継装置の鍵情報エリア8a1は、中継装置管理者のログインID、および、中継装置と第3者機関との共通鍵が登録される項目欄8a1a、8a1bから構成されている。

【0027】図7は、図5の鍵管理テーブルにおける任意のユーザの鍵情報エリアの詳細な構成例を示す説明図である。任意のユーザ(x)の鍵情報エリア8a2xは、ユーザ(x)のログインID、および、ユーザ(x)と中継装置との共通鍵が登録される項目欄8a2x1、8a2x2から構成されている。

【0028】図8は、図5の鍵管理テーブルにおける任意のマーチャントの鍵情報エリアの詳細な構成例を示す説明図である。任意のマーチャント(x)の鍵情報エリア8a3xは、マーチャント(x)のログインID、および、マーチャント(x)と中継装置との共通鍵が登録される項目欄8a3x1、8a3x2から構成されている。

【0029】図9は、図2における受信側計算機の鍵管理テーブルの詳細な構成例を示す説明図である。図2における計算機4の鍵管理テーブル4hには、マーチャント(1)鍵情報、マーチャント(2)鍵情報、マーチャント(3)鍵情報、・・・、マーチャント(m)鍵情報等の、計算機4の各マーチャント毎のログインIDと各共通鍵が登録される鍵情報エリア(領域)4h1～4hmが設けられている。

【0030】図10は、図9の鍵管理テーブルにおける任意のマーチャントの鍵情報エリアの詳細な構成例を示す説明図である。一つの鍵情報エリア4hxは、それぞれ、マーチャント(x)のログインID、マーチャント(x)と第3者機関の共通鍵、マーチャント(x)と中継装置の共通鍵が登録される項目欄4hx1～4hx3から構成されている。

【0031】図11は、図2における送信側計算機のコネクション管理テーブルの詳細な構成例を示す説明図である。図2における計算機1のコネクション管理テーブル

1 i には、ユーザ側コネクション (1) 情報、ユーザ側コネクション (2) 情報、ユーザ側コネクション (3) 情報、・・・、ユーザ側コネクション (i) 情報等の、計算機 1 の各ユーザのコネクション毎に、次の図 1 2 で示す各情報が登録される情報エリア 1 i 1 ~ 1 i j が設けられている。

【0032】図 1 2 は、図 1 1 のコネクション管理テーブルにおける任意のユーザ側コネクションの情報エリアの詳細な構成例を示す説明図である。一つの情報エリア 1 i x は、ユーザ側のコネクション ID と、ユーザ (x) のログイン ID、ユーザ (x) と中継装置との共通鍵、マーチャント (y) の名前、状態遷移表の状態が登録される項目欄 1 i x 1 ~ 1 i x 5 から構成されている。尚、本例では、自分および通信相手（ここでは中継装置）の各レイヤの通信エンティティのサービスアクセスポイントは省略している。これは、以降で説明する図 1 4、図 1 6 でも同様である。

【0033】図 1 3 は、図 2 における受信側計算機のコネクション管理テーブルの詳細な構成例を示す説明図である。図 2 における計算機 4 のコネクション管理テーブル 4 i には、マーチャント側コネクション (1) 情報、マーチャント側コネクション (2) 情報、マーチャント側コネクション (3) 情報、・・・、マーチャント側コネクション (j) 情報等の、計算機 4 の各マーチャントのコネクション毎に、次の図 1 4 で示す各情報が登録される情報エリア 4 i 1 ~ 4 i j が設けられている。

【0034】図 1 4 は、図 1 3 のコネクション管理テーブルにおける任意のマーチャント側コネクションの情報エリアの詳細な構成例を示す説明図である。一つの情報エリア 4 i x は、マーチャント側のコネクション ID と、マーチャント (x) のログイン ID、マーチャント (x) と中継装置との共通鍵、状態遷移表の状態が登録される項目欄 4 i x 1 ~ 4 i x 4 から構成されている。

【0035】図 1 5 は、図 2 における中継装置のコネクション管理テーブルの詳細な構成例を示す説明図である。図 2 における中継装置 7 のコネクション管理テーブル 7 i には、次の図 1 6 で示す各中継情報 (1) ~ (j) が登録される情報エリア 7 i 1 ~ 7 i j が設けられている。

【0036】図 1 6 は、図 1 5 のコネクション管理テーブルにおける任意の情報エリアの詳細な構成例を示す説明図である。一つの情報エリア 7 i x は、ユーザ側コネクション ID、ユーザ (x) のログイン ID、ユーザ (x) と中継装置との共通鍵、マーチャント側のコネクション ID、マーチャント (y) のログイン ID、マーチャント (y) と中継装置との共通鍵、状態遷移表の状態がそれぞれ登録される項目欄 7 i x 1 ~ 7 i x 7 から構成されている。

【0037】図 1 7 は、図 2 における中継装置のユーザ名／マーチャント名変換テーブルの詳細な構成例を示す

説明図である。図 2 における中継装置 7 のユーザ名／マーチャント名変換テーブル 7 k には、各マーチャント (1) ~ (m) の名前とログイン ID、および、各ユーザ (1) ~ (n) の名前とログイン ID とが対応付けて登録される情報エリア 7 k 1 a ~ 7 k 1 m, 7 k 2 a ~ 7 k 2 n が設けられている。

【0038】次に、図 1 8 ~ 図 2 0 の各フローチャートにより、図 2 における中継装置 7 を用いた暗号通信システムでの暗号通信の動作を説明する。尚、図 1 8 ~ 2 0 の各フローチャートは、図 2 における計算機 1 から中継装置 7 へ、また、中継装置 7 から計算機 4 へコネクション確立要求をすることを前提としている。図 1 8 は、図 2 における送信側計算機の暗号通信処理部による動作例を示すフローチャートである。まず、イベントの生起を待ち（ステップ 1 8 0 2）、外部イベントがあると（ステップ 1 8 0 3）、メッセージを復号化し（ステップ 1 8 1 0）、イベントを判定する（ステップ 1 8 1 1）。その後、まだ処理があるか判断する（ステップ 1 8 1 2）。

【0039】また、ステップ 1 8 0 3 でのイベントが内部イベントであれば、まず、イベントの判定を行う（ステップ 1 8 0 4）。イベントが、図 2 における業務処理部 1 d からのコネクション確立要求であれば（ステップ 1 8 0 5）、ユーザのログイン ID をシステムファイルから読み取り（ステップ 1 8 0 6）、今確立するコネクションと同じユーザログイン ID とマーチャント名の属性を持つコネクションが存在するか否かを判断する（ステップ 1 8 0 7）。存在すれば、図 2 における既存のコネクション管理テーブル 1 i を使用し（ステップ 1 8 0 8）、存在しなければ、新たにコネクション ID を生成し、図 2 のコネクション管理テーブル 1 i に、図 1 2 に示すユーザ側コネクション情報エリア 1 i x を新しく生成し、このエリアに対応する値をセットする（ステップ 1 8 0 9）。

【0040】その後、ステップ 1 8 1 2 での未だ処理があるか否かの判断を行う。また、ステップ 1 8 0 5 において、イベントが、図 2 における業務処理部 1 d からのコネクション確立要求でなければ、直ちに、ステップ 1 8 1 2 における未だ処理があるかの判断を行う。各ステップ 1 8 0 5, 1 8 0 8, 1 8 0 9, 1 8 1 1 での処理の後でのステップ 1 8 1 2 における判断の結果、未だ処理があつて、かつ、その結果がコネクション確立要求送信であれば（ステップ 1 8 1 4）、メッセージにユーザ名、コネクション ID、マーチャント名をセットする（ステップ 1 8 1 5）。また、ステップ 1 8 1 4 において、コネクション確立要求以外のメッセージの送信であれば、メッセージにコネクション ID をセットする（ステップ 1 8 1 6）。

【0041】ステップ 1 8 1 5, 1 8 1 6 の後、メッセージを暗号化して（ステップ 1 8 1 7）、送信する（ス

ステップ1818)。その後、ステップ1812の処理に戻り、未だ処理があるか否かを判断する。もし、ステップ1812での判断で、次の処理がないとの結果であれば、状態遷移先を図12の状態遷移表の状態エリア1 i x 5にセットし(ステップ1813)、ステップ1802のイベント生起待ちの処理に戻る。このようにして、図2の計算機1の暗号通信処理部1 eは、メッセージの暗号化と送信等を行う。

【0042】図19は、図2における中継装置の暗号通信処理部による動作例を示すフローチャートである。まず、イベントの生起を待つ(ステップ1902)。内部イベントがあれば(ステップ1903)、イベントを判定し(ステップ1904)、その後、未だ処理があるか否かを判断する(ステップ1911)。また、ステップ1903で外部イベントを判別すれば、メッセージを復号化し(ステップ1905)、イベントが何かを判定する(ステップ1906)。

【0043】イベントがユーザからのコネクション確立要求であれば(ステップ1907)、メッセージ中のコネクションIDと同じコネクションIDが、図2におけるコネクション管理テーブル7 iの、図16に示すユーザ側コネクションIDエリア7 i x 1にあるか否かを判断する(ステップ1908)。なければ、新たにマーチャント側コネクションIDを生成し、図2のコネクション管理テーブル7 iに、図16に示す中継情報エリア7 i xを新しく生成し、対応する値をセットする(ステップ1909)。その後、未だ処理があるか判断する(ステップ1911)。

【0044】また、ステップ1908において、メッセージ中のコネクションIDと同じコネクションIDがユーザ側コネクションIDエリア1601にあれば、図2に示す既存のコネクション管理テーブル7 iを使用する(ステップ1910)。その後、ステップ1911における未だ処理があるか否かの判断を行う。また、ステップ1907において、イベントがユーザからのコネクション確立要求でなければ、直ちに、ステップ1911における処理に進み、未だ処理があるかを判断する。

【0045】各ステップ1904、1907、1909、1910での処理の後でのステップ1911における判断の結果、未だ処理があれば、その処理がコネクション確立要求送信か否かを判断する(ステップ1913)。コネクション確立要求送信であれば、メッセージに、マーチャント側コネクションIDとマーチャント名をセットし(ステップ1914)、メッセージを暗号化し(ステップ1916)、送信する(ステップ1917)。その後、未だ処理があるかの判断に戻る(ステップ1911)。

【0046】また、ステップ1913での判断の結果が、コネクション確立要求以外の送信であれば、メッセージにマーチャント側コネクションIDをセットし(ス

テップ1915)、メッセージを暗号化し(ステップ1916)、送信する(ステップ1917)。また、ステップ1911での判断の結果、処理がもうなければ、状態遷移先を図16に示す状態遷移表の状態エリア7 i x 7にセットし(ステップ1912)、ステップ1902におけるイベント生起待ちの処理に戻る。このようにして、図2の中継装置7の暗号通信処理部1 eは、メッセージの暗号化と送信等を行う。

【0047】図20は、図2における受信側計算機の暗号通信処理部による動作例を示すフローチャートである。まず、イベントの生起を待つ(ステップ2002)。イベントが内部イベントであれば(ステップ2003)、イベントを判定し(ステップ2004)、未だ処理があるか判断する(ステップ2013)。また、ステップ2003の判断において、イベントが外部イベントであれば、メッセージを復号化し(ステップ2005)、イベントが何かを判定する(ステップ2006)。

【0048】イベントが、図2における中継装置7からのコネクション確立要求であれば(ステップ2007)、メッセージ中のマーチャント側コネクションIDと同じコネクションIDが、図14に示すマーチャント側コネクションIDエリア4 i x 1にあるか否かを判断する(ステップ2008)。あれば、当該マーチャントがログインしているか判断し(ステップ2009)、ログインしていれば、図2における既存のコネクション管理テーブル4 iを使用し(ステップ2011)、未だ処理があるか判断する(ステップ2013)。ステップ2009において、ログインしていなければ、当該コネクション確立要求を捨てて(ステップ2010)、ステップ2002に戻り、イベント生起待ちとなる。

【0049】また、ステップ2008において、メッセージ中のマーチャント側コネクションIDと同じコネクションIDが無ければ、図2のコネクション管理テーブル4 iに、新たに図14に示すマーチャント側コネクション情報エリア4 i xを生成し、対応する値をセットする(ステップ2012)。その後、未だ処理があるかの判断を行なう(ステップ2013)。また、ステップ2007において、イベントがコネクション確立要求でなければ、直ちに、未だ処理があるか否かの判断を行なう(ステップ2013)。

【0050】各ステップ2004、2007、2011、2012での処理の後でのステップ2013における判断の結果、未だ処理があれば、メッセージにマーチャント側コネクションIDをセットし(ステップ2015)、メッセージを暗号化し(ステップ2016)、送信する(ステップ2017)。その後、ステップ2013に戻り、未だ処理があるかの判断を行う。ステップ2013における判断結果で、もう処理がなければ、状態遷移先を図14に示す状態遷移表の状態エリア4 i x 4に

セットし（ステップ2014）、ステップ2002のイベント生起待ちの処理に戻る。このようにして、受信側計算機である図2の計算機4の暗号通信処理部4eは、メッセージの暗号化と送信等を行う。

【0051】次に、図21を用いて、複数の中継装置を設けた場合での暗号通信システムの本発明に係る構成例および処理動作例を説明する。図21は、複数の中継装置を設けた本発明の暗号通信システムの構成例を示すブロック図である。本例では、二つの中継装置7A、7Bを設けており、それぞれの中継装置7A、7Bは、一サービスパロバイダにより運用されている。また、各中継装置7A、7Bは、共有メモリ9に結合され、この共有メモリ9に全てのユーザやマーチャントの共通鍵をおき、各中継装置7A、7Bで使用する。このことにより、中継装置7A、7Bのいずれにおいても、各計算機1～6間での暗号通信の中継を行うことができる。

【0052】また、本例では、各中継装置7A、7Bの受信側計算機4～6とのそれぞれの接続管理を行う接続管理装置10を設けている。この接続管理装置10では、中継装置7A、7Bの計算機4～6との通信量に基づき、中継装置7A、7Bのそれぞれの通信量が平準化するように接続の組み合わせを切替る。例えば、本例では、中継装置7Aと計算機4、5が、また、中継装置7Bと計算機6が接続されており、各中継装置7A、7Bとの通信量は、計算機4が1000bps、計算機5が200bps、計算機6が500bpsであれば、最も通信量の少ない計算機5の回線を中継装置7Bに接続する。このように、回線の接続を切替る場合、少ない通信量の回線を優先的に選択することにより、切替に要する処理負荷を軽減することができる。尚、この時、計算機5と通信する計算機1～3は、中継装置7Bに接続する。

【0053】また、接続管理装置10は、中継装置7A、7Bと計算機4～6との接続状況を管理しているので、この接続状況に基づき、送信側の計算機1～3が接続したい受信側の計算機4～6が接続されている中継装置7A、7Bに、計算機1～3を正しく接続することができる。また、送信側の計算機1では、ICカード11を読み取るカードリーダー12を有しており、計算機1のユーザは、共通鍵をICカード11に入れておく。そして、ICカード11から共通鍵をカードリーダー12に読ませて計算機1に入力する。このことにより、ユーザ側での鍵管理をさらに容易にすることができる。

【0054】以上、図1～図21を用いて説明したように、本実施例の暗号通信システムでは、お互いに暗号通信をする計算機1、4の間に、その通信を中継する暗号通信中継装置としての中継装置7を導入し、この中継装置7が共通鍵を保持し、送信側計算機1からの暗号化メッセージを復号化し、受信側計算機4との共通鍵で暗号化して受信側計算機4に送信する。このことにより、各

計算機1、4（ユーザおよびマーチャントの相方）は、中継装置7との共通鍵のみを持てば良くなり、ユーザの鍵の取扱いが容易、かつ迅速になる。また、鍵保管のためのメモリ容量が小さくなる。さらに、通信の必要発生時に、暗号鍵を得る技術と比較して、暗号通信完了までの時間を短くすることができる。

【0055】尚、本発明は、図1～図21を用いて説明した実施例に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能である。例えば、図21での構成では、共有メモリで全ての鍵情報を一元的に管理しているが、各計算機に同じ暗号鍵を保持させることによって、任意の中継装置で、各計算機間での暗号通信の中継を行なうこともできる。

【0056】

【発明の効果】本発明によれば、高速な暗号通信をする送信側計算機での煩雑な鍵の取り扱いが不要となり、かつ、鍵保管のためのメモリ容量の消費を回避でき、多数の計算機間での暗号通信に要する鍵管理を効率良く行うことができ、暗号通信システムの利便性を含むトータルな性能の向上を図ることが可能である。

【図面の簡単な説明】

【図1】本発明の暗号通信システムおよび暗号通信中継装置の本発明に係る構成の一実施例を示すブロック図である。

【図2】図1における計算機と中継装置および第三者機関のそれぞれの内部構成例を示すブロック図である。

【図3】図2における発信側計算機の鍵管理テーブルの詳細な構成例を示す説明図である。

【図4】図3の鍵管理テーブルにおける任意のユーザの鍵情報エリアの詳細な構成例を示す説明図である。

【図5】図2における中継装置の鍵管理テーブルの詳細な構成例を示す説明図である。

【図6】図5の鍵管理テーブルにおける中継装置の鍵情報エリアの詳細な構成例を示す説明図である。

【図7】図5の鍵管理テーブルにおける任意のユーザの鍵情報エリアの詳細な構成例を示す説明図である。

【図8】図5の鍵管理テーブルにおける任意のマーチャントの鍵情報エリアの詳細な構成例を示す説明図である。

【図9】図2における受信側計算機の鍵管理テーブルの詳細な構成例を示す説明図である。

【図10】図9の鍵管理テーブルにおける任意のマーチャントの鍵情報エリアの詳細な構成例を示す説明図である。

【図11】図2における送信側計算機の接続管理テーブルの詳細な構成例を示す説明図である。

【図12】図11の接続管理テーブルにおける任意のユーザ側接続の情報エリアの詳細な構成例を示す説明図である。

【図13】図2における受信側計算機の接続管理

理テーブルの詳細な構成例を示す説明図である。

【図14】図13のコネクション管理テーブルにおける任意のマーチャント側コネクションの情報エリアの詳細な構成例を示す説明図である。

【図15】図2における中継装置のコネクション管理テーブルの詳細な構成例を示す説明図である。

【図16】図15のコネクション管理テーブルにおける任意の情報エリアの詳細な構成例を示す説明図である。

【図17】図2における中継装置のユーザ名／マーチャント名変換テーブルの詳細な構成例を示す説明図である。

【図18】図2における送信側計算機の暗号通信処理部による動作例を示すフローチャートである。

【図19】図2における中継装置の暗号通信処理部による動作例を示すフローチャートである。

【図20】図2における受信側計算機の暗号通信処理部による動作例を示すフローチャートである。

【図21】複数の中継装置を設けた本発明の暗号通信システムの構成例を示すブロック図である。

【符号の説明】

1～6：計算機、1a、2a～6a、7a：表示装置、1b、2b～6b、7b：入力装置、1c：メール処理部、1d：業務処理部、1e：暗号通信処理部、1f：暗号化部、1g：復号化部、1h：鍵管理テーブル、1

i：コネクション管理テーブル、1j：OS、4c：メール処理部、4d：業務処理部、4e：暗号通信処理部、4f：復号化部、4g：復号化部、4h：鍵管理テーブル、4i：コネクション管理テーブル、4j：OS、4k：マーチャント名変換テーブル、7、7A、7B：中継装置、7c：メール処理部、7e：暗号通信処理部、7f：暗号化部、7g：復号化部、7h：鍵管理テーブル、7i：コネクション管理テーブル、7j：OS、7k：ユーザ名／マーチャント名変換テーブル、8：第3者機関、8a：鍵管理テーブル、8b：証明書作成部、8c：メール処理部、9：共有メモリ、10：接続管理装置、11：ICカード、12：カードリーダー、1h1～1hn、1hx：鍵情報エリア、1hx1～1hx3：項目欄、1i1～1ij、1ix：情報エリア、1ix1～1ix5：項目欄、4h1～4hm、4hx：鍵情報エリア、4hx1～4hx3：項目欄、4i1～4ij、4ix：情報エリア、4ix1～4ix4：項目欄、7i1～7ij、7ix：情報エリア、7ix1～7ix7：項目欄、7k1a～7k1m、7k2a～7k2n：情報エリア、8a1、8a2a～8a2n、8a3a～8a3m、8a2x、8a3x：鍵情報エリア、8a1a、8a1b、8a2x1、8a2x2、8a3x1、8a3x2：項目欄。

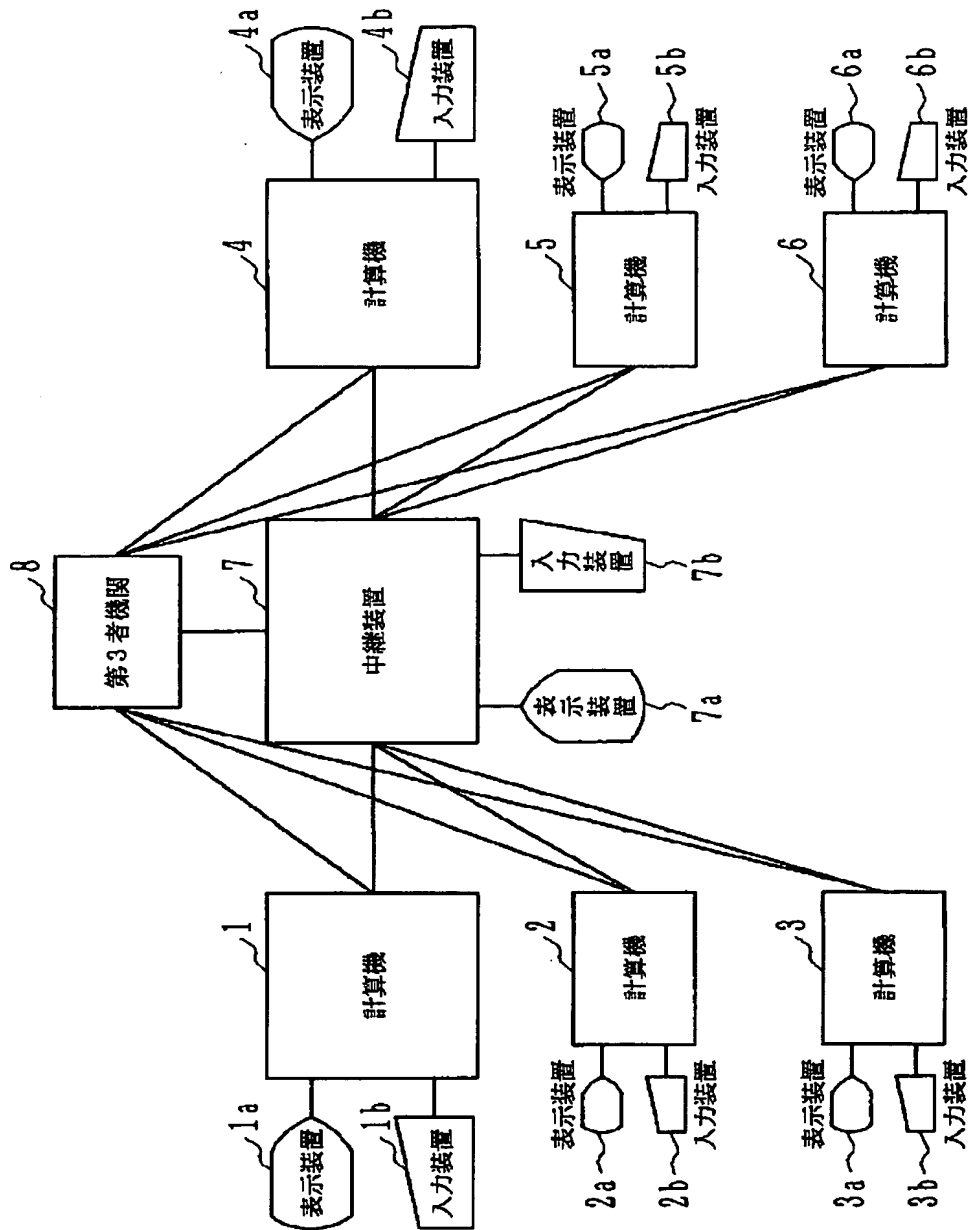
【図3】

計算機1の鍵管理テーブル		1h
ユーザ(1)鍵情報	1h1	
ユーザ(2)鍵情報	1h2	
ユーザ(3)鍵情報	1h3	
ユーザ(n)鍵情報		1hn

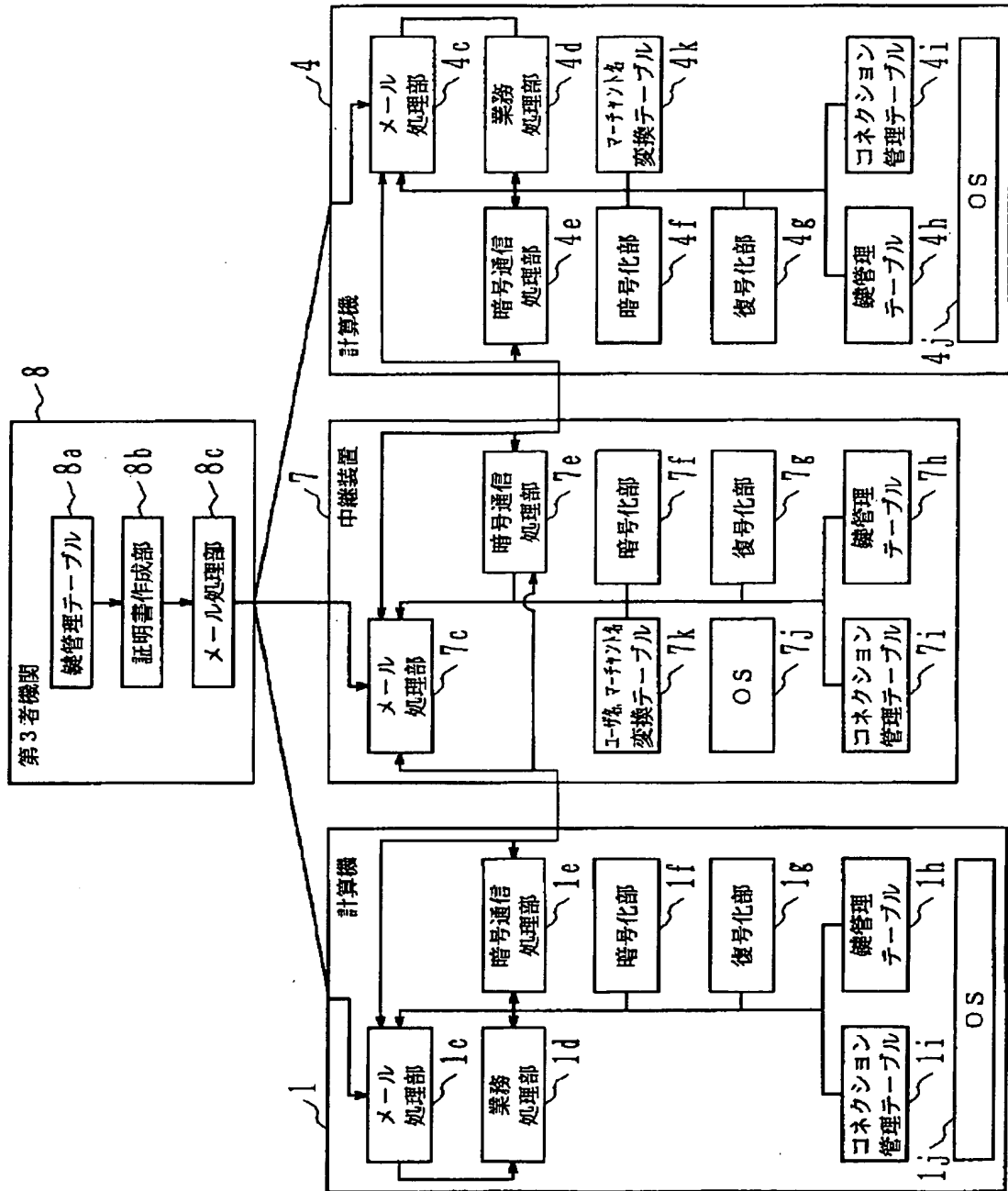
【図17】

ユーザ名／マーチャント名変換テーブル		7k
マーチャント1の名前	マーチャント1のログインID	7k1a
マーチャント2の名前	マーチャント2のログインID	7k1b
マーチャント3の名前	マーチャント3のログインID	7k1c
マーチャントmの名前	マーチャントmのログインID	7k1n
ユーザ1の名前	ユーザ1のログインID	7k2a
ユーザ2の名前	ユーザ2のログインID	7k2b
ユーザ3の名前	ユーザ3のログインID	7k2c
ユーザnの名前	ユーザnのログインID	7k2n

【図1】



【図2】



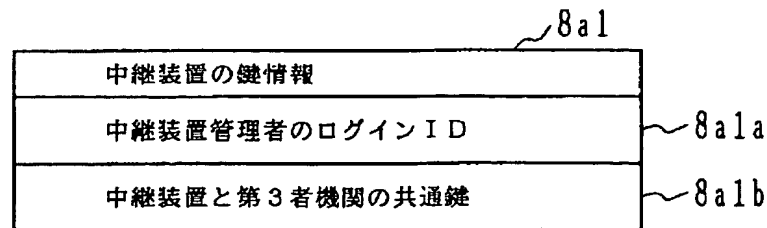
【図4】

1hx	
ユーザ(x)鍵情報	
ユーザ(x)のログインID	1hx1
ユーザ(x)と第3者機関の共通鍵	1hx2
ユーザ(x)と中継装置の共通鍵	1hx3

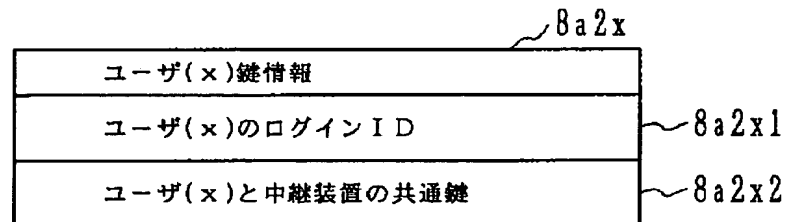
【図5】

8a	
中継装置7の鍵管理テーブル	
中継装置の鍵情報	8a1
ユーザ(1)鍵情報	8a2a
ユーザ(2)鍵情報	8a2b
ユーザ(3)鍵情報	8a2c
ユーザ(n)鍵情報	8a2n
マーチャント(1)鍵情報	8a3a
マーチャント(2)鍵情報	8a3b
マーチャント(3)鍵情報	8a3c
マーチャント(m)鍵情報	8a3m

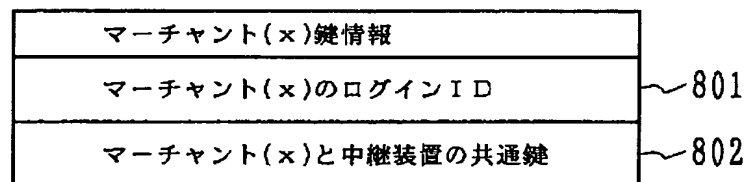
【図6】



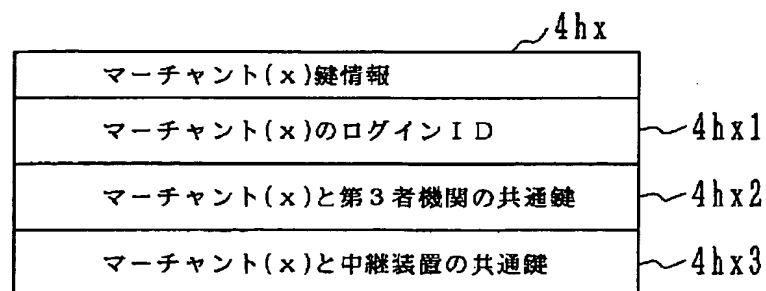
【図7】



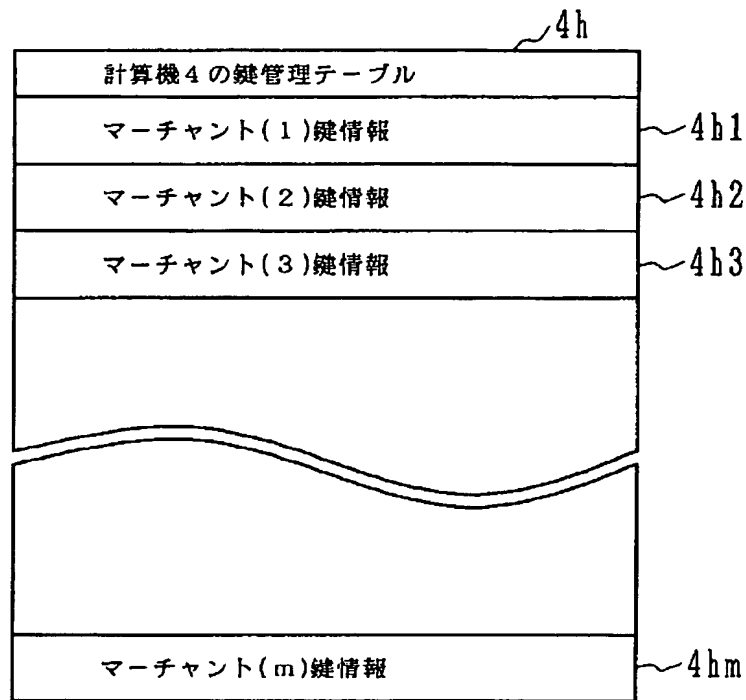
【図8】



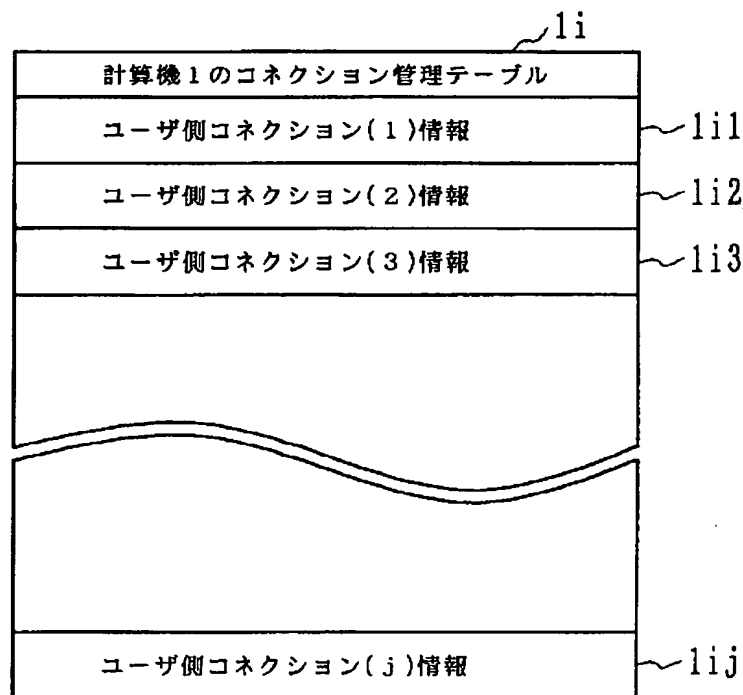
【図10】



【図9】



【図11】



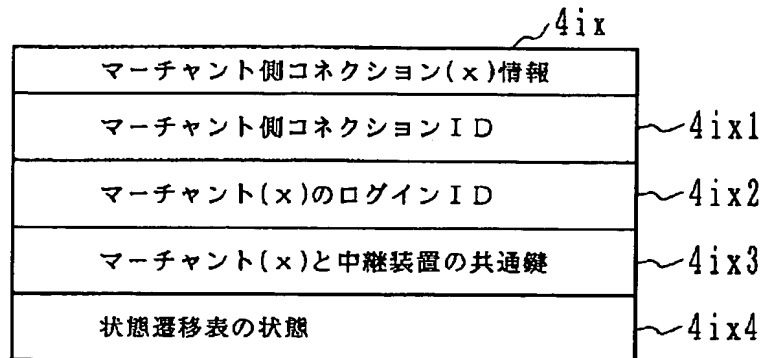
【図12】

lix	
ユーザ側コネクション(x)情報	
ユーザ側コネクションID	lix1
ユーザ(x)のログインID	lix2
ユーザ(x)と中継装置の共通鍵	lix3
マーチャント(y)の名前	lix4
状態遷移表の状態	lix5

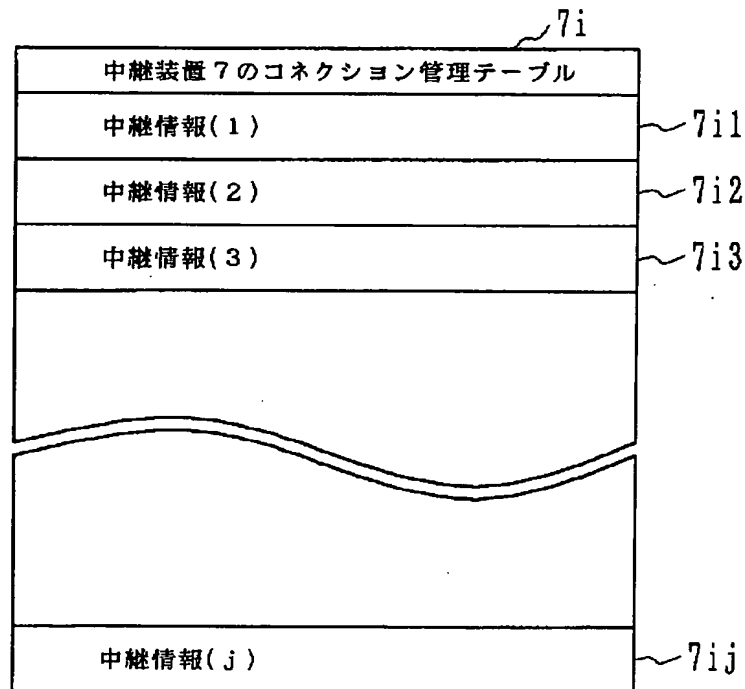
【図13】

4i	
計算機4のコネクション管理テーブル	
マーチャント側コネクション(1)情報	4i1
マーチャント側コネクション(2)情報	4i2
マーチャント側コネクション(3)情報	4i3
マーチャント側コネクション(j)情報	4ij

【図14】



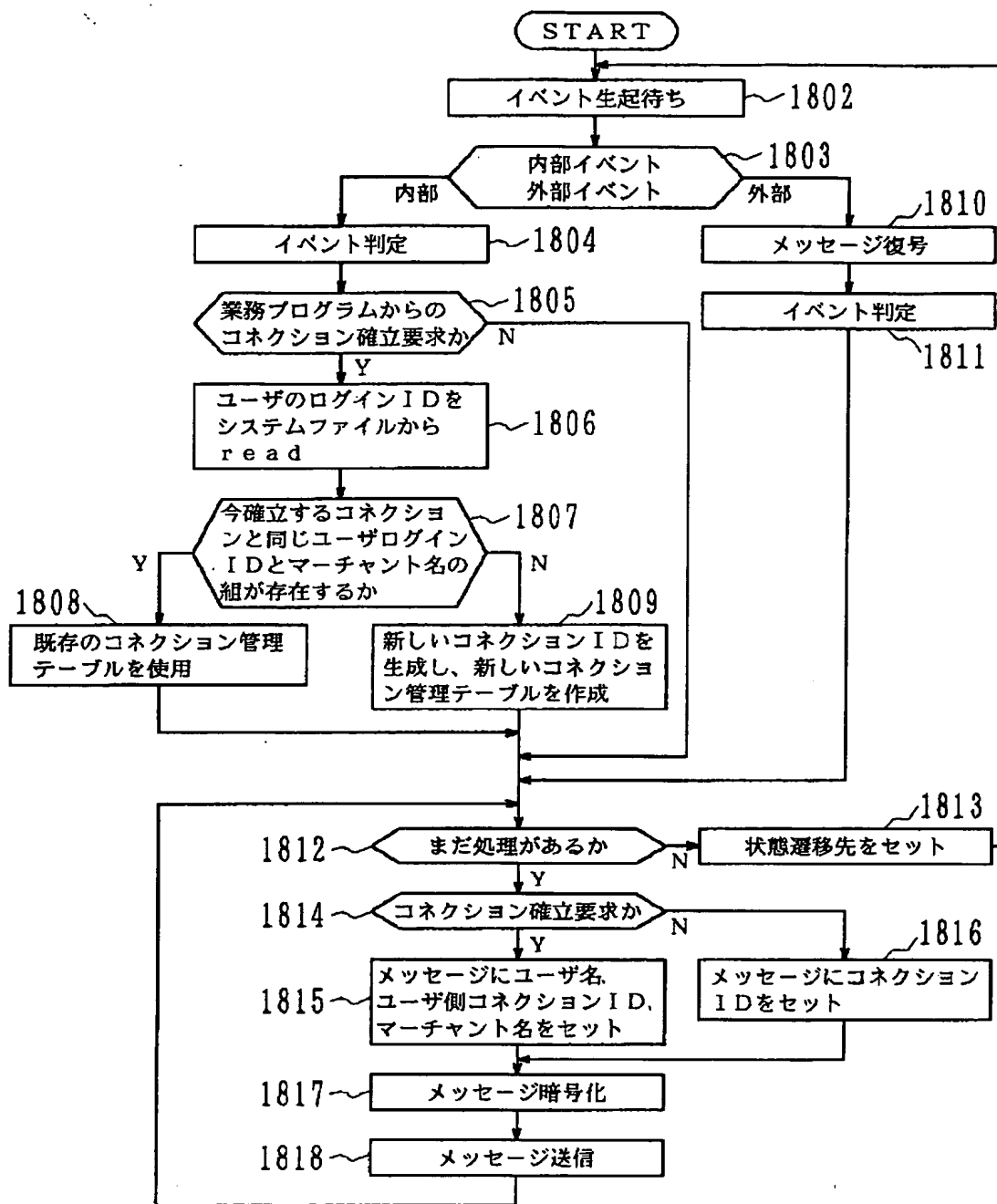
【図15】



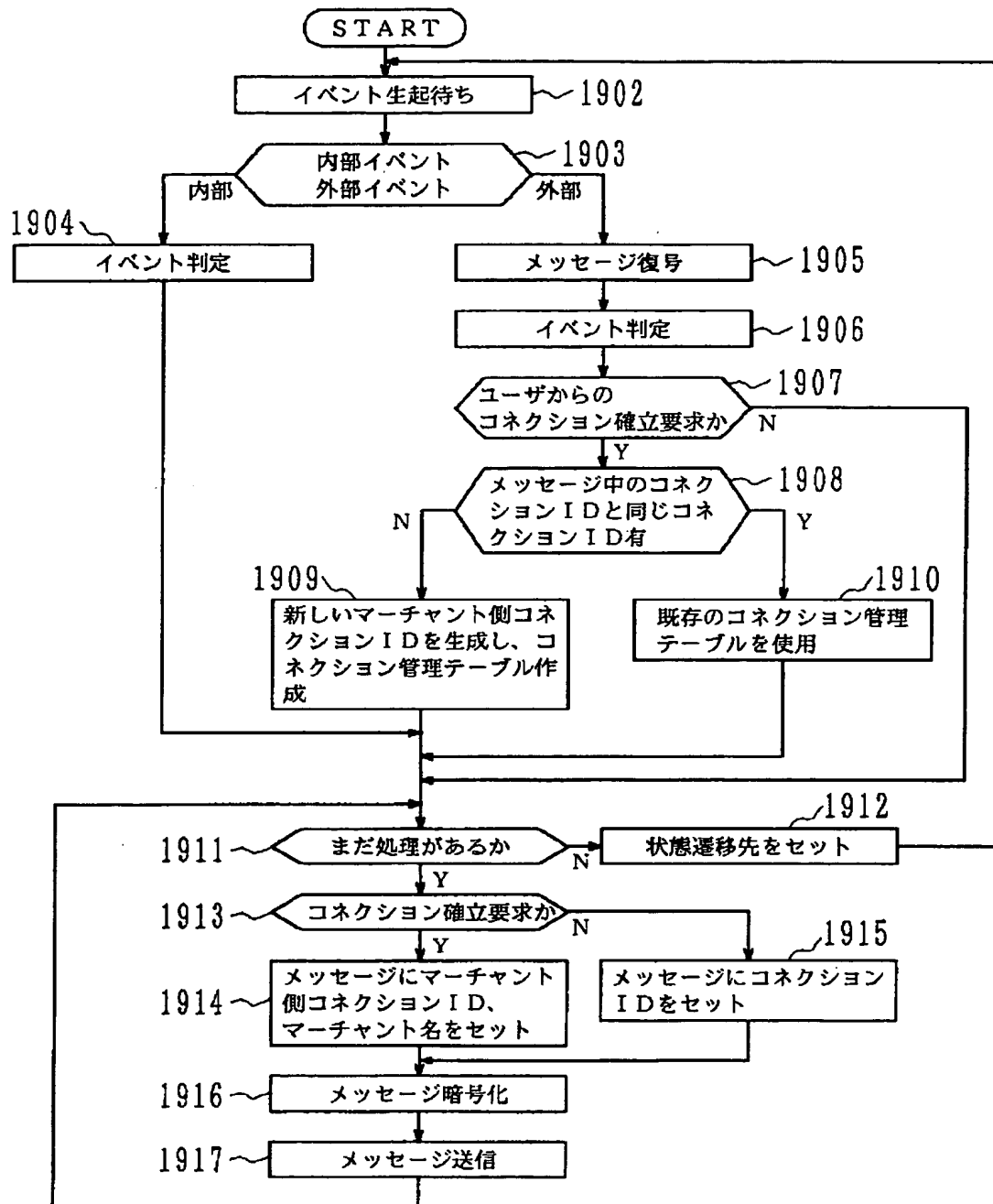
【図16】

中継情報(x)		7ix
ユーザ側コネクションID	7ix1	
ユーザ(x)のログインID	7ix2	
ユーザ(x)と中継装置の共通鍵	7ix3	
マーチャント側コネクションID	7ix4	
マーチャント(y)のログインID	7ix5	
マーチャント(y)と中継装置の共通鍵	7ix6	
状態遷移表の状態	7ix7	

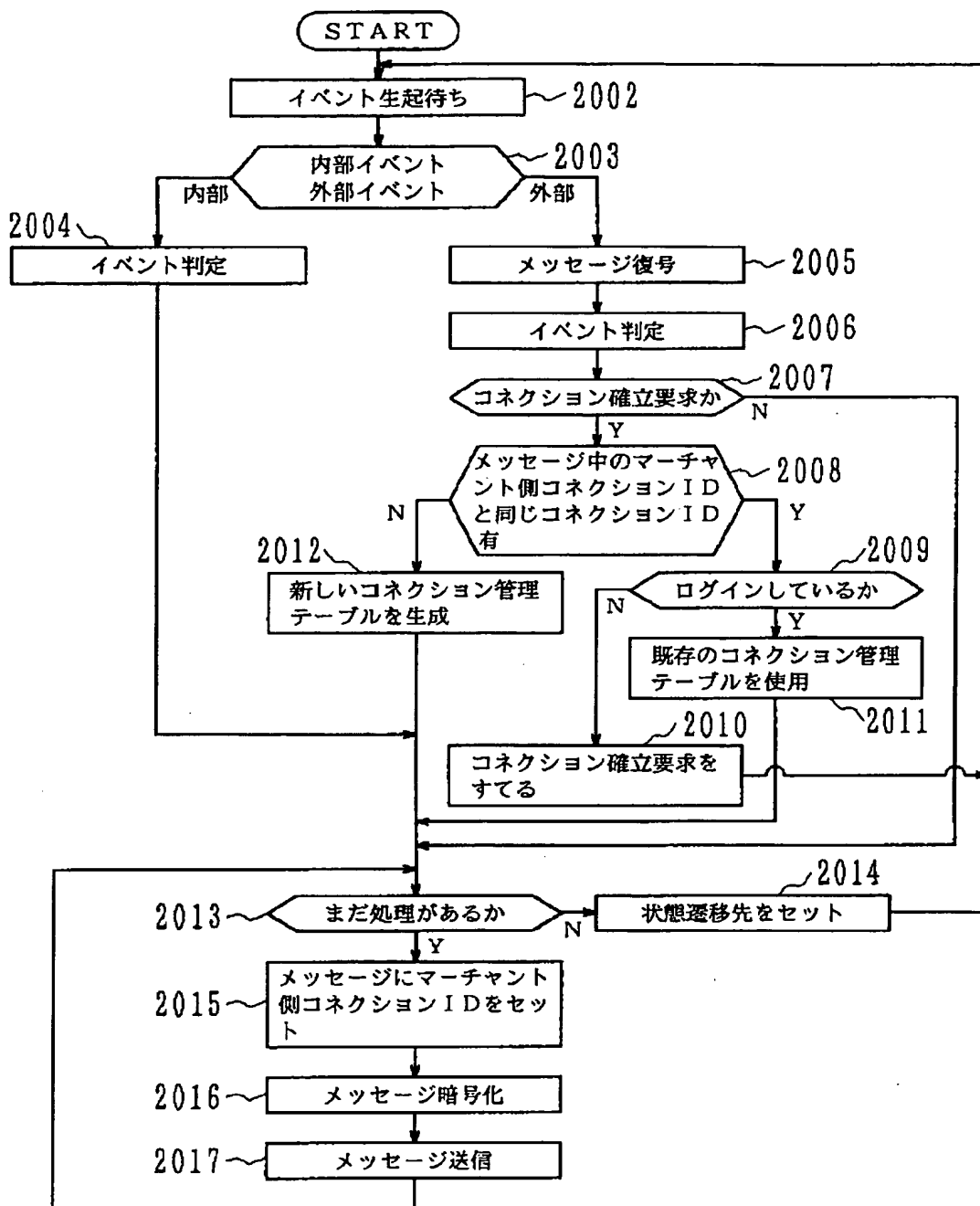
【図18】



【図19】



【図20】



【図21】

